Όνομα: ΑΜ:

Κρυπτογραφία – Γραπτή εξέταση Ιουνίου 2019

Οδηγίες: Απαντήστε και τα 4 (τέσσερα) θέματα. Δεν επιτρέπονται σημειώσεις ή υπολογιστικές συσκευές. Τα θέματα είναι ισοδύναμα. Μέγιστη βαθμολογία είναι το 120. Στις απαντήσεις σας να είστε σαφείς, να εξηγείτε τη σκέψη σας, και να απαντάτε στο ζητούμενο. Πριν αρχίσετε να λύνετε, διαβάστε όλα τα θέματα. Για τους μεταπτυχιακούς υπάρχουν επιπλέον ερωτήματα με κατάλληλη ένδειξη.

Θέμα 1. Θεωρήστε ένα 3-out-of-n σχήμα διαμοίρασης μυστικού του Shamir στο $\mathbb{Z}_{17}$, όπου ο παίκτης i λαμβάνει μερίδιο $y_i = P(i)$ (όπου $P(x)$ το πολυώνυμο μου επέλεξε ο διαμοιραστής). Οι παίκτες $2, 5, 10$ έλαβαν μερίδια $1, 1, 2$, αντίστοιχα.

(α΄) Υπολογίστε το μυστικό. Για την παρεμβολή Lagrange δίνεται ο τύπος των συντελεστών λ_i, όπου $\lambda_i := \prod_{j \neq i}(x - j)/(i - j)$. Δείξτε αναλυτικά τους υπολογισμούς σας.

[Μονάδες: 15 (Μεταπτυχιακοί: 10)]

(β΄) Είναι δυνατό να ενταχθούν στο σχήμα παίκτες με δείκτη 0 ή -1; Εξετάστε τις περιπτώσεις ξεχωριστά και εξηγήστε την απαντησή σας.

[Μονάδες: 15 (Μεταπτυχιακοί: 10)]

(γ΄) **Μόνο Μεταπτυχιακοί.** Εστω ότι ένας νέος παίκτης (με αριθμό-δείκτη το 16) θέλει να ενταχθεί στο σχήμα. Ο διαμοιραστής (dealer) δεν είναι διαθέσιμος. Με δεδομένο ότι οι παίκτες είναι τίμιοι, εξηγήστε πως οι παίκτες $2, 5, 10$ μπορούν να στείλουν στον νέο παίκτη αρκετές πληροφορίες ώστε να υπολογίσει το μεριδιό του. Στη λύση σας δεν επιτρέπεται κάποιος παίκτης να είναι σε θέση να παράξει το μυστικό. Θεωρήστε ότι είναι εφικτό οι παίκτες να στέλνουν προσωπικά μηνύματα ο ένας στον άλλο.

[Μονάδες: 10 (Μόνο μεταπτυχιακοί)]

Θέμα 2. (α΄) Να δώσετε τον ορισμό της Στατιστικής Απόστασης ανάμεσα σε δύο κατανομές.

[Μονάδες: 10]

(β΄) Έστω κυκλική ομάδα $\mathbb{G} = \langle g \rangle$ τάξης q, όπου q πρώτος μήκους λ bits. Να υπολογίσετε την στατιστική απόσταση ανάμεσα στις παρακάτω κατανομές:

$$\mathcal{D}_\lambda := \left\{ a, b \xleftarrow{\text{r}} \mathbb{Z}_q \colon (g^a, g^b, g^{ab}) \right\}$$
$$\mathcal{R}_\lambda := \left\{ a, b, c \xleftarrow{\text{r}} \mathbb{Z}_q \colon (g^a, g^b, g^c) \right\}$$

[Μονάδες: 10]

(γ΄) Να διατυπώσετε την υπόθεση DDH και να εξηγήσετε εάν είναι συμβατή με τον παραπάνω υπολογισμό σας.

[Μονάδες: 10]

Όνομα: ΑΜ:

Θέμα 3. (α΄) Έστω $\langle \mathcal{P}, \mathcal{V} \rangle$ ένα ζεύγος αλληλεπιδρόντων προγραμμάτων. Ορίζουμε ως $\text{out}^{\mathcal{P}}_{\mathcal{P},\mathcal{V}}(x, w, z)$ να είναι η έξοδος του $\mathcal{P}$ όταν οι $\mathcal{P}$ και $\mathcal{V}$ εκτελούνται με τη δημόσια είσοδο x και τις ιδιωτικές εισόδους w και z (ο $\mathcal{P}$ δέχεται τα x, w και ο $\mathcal{V}$ τα x, z). Το $\text{out}^{\mathcal{V}}_{\mathcal{P},\mathcal{V}}$ ορίζεται όμοια για το $\mathcal{V}$.

Να ορίσετε πότε ένα διαδραστικό πρωτόκολλο $\langle \mathcal{P}, \mathcal{V} \rangle$ είναι μια ***απόδειξη μηδενικής γνώσης (zero-knowledge proof)*** για μία γλώσσα $\mathcal{L}_R = \{x | \exists w : R(x, w) = 1\}$ (όπου R πολυωνυμικός αλγόριθμος με έξοδο στο $\{0, 1\}$) δίνοντας τις τρεις ιδιότητες :

- Πληρότητα (completeness)
- Εγκυρότητα (soundness)
- Μηδενική γνώση (zero-knowledge)

Για κάθε ιδιότητα να δώσετε ορισμό ακολουθώντας τους παραπάνω συμβολισμούς. Επίσης να εξηγήσετε τι σημαίνει η ιδιότητα μηδενικής γνώσης για τίμιους επαληθευτές (honest verifier zero-knowledge).

[Μονάδες: 15 (Μεταπτυχιακοί: 10)]

(β΄) Δίνεται μια παραλλαγή του πρωτοκόλλου των Chaum και Pedersen, με το οποίο θέλουμε να να αποδείξουμε την ισότητα δύο διακριτών λογαρίθμων, δηλαδή οτι κάποια πρόταση της μορφής $\langle \langle \mathbb{G}, g_1, g_2, q \rangle, h_1, h_2 \rangle$ ανήκει στη γλώσσα EQDLOG $:= \{\langle \langle \mathbb{G}, g_1, g_2, q \rangle, h \rangle : h_1 = g_1^w \cap h_2 = g_2^w$ για κάποιο $w \in \mathbb{Z}_q\}$ χωρίς να φανερώσουμε το $w = \log_{g_i} h_i$.

i. Ο $\mathcal{P}$ διαλέγει $t \xleftarrow{\text{r}} \mathbb{Z}_q$ και στέλνει τα $y_1 = g_1^t, y_2 = g_2^t$ στον $\mathcal{V}$.

ii. Ο $\mathcal{V}$ διαλέγει μια πρόκληση $c \xleftarrow{\text{r}} \mathbb{Z}_q$ και την στέλνει στον $\mathcal{P}$.

iii. Ο $\mathcal{P}$ υπολογίζει το $s = t + w + c \bmod q$ και στέλνει το s στον $\mathcal{V}$.

iv. Ο $\mathcal{V}$ ελέγχει και αποδέχεται αν και μόνο αν $g_1^s = y_1 h_1 g_1^c$ και $g_2^s = y_2 h_2 g_2^c$.

Να εξετάσετε το παραπάνω πρωτόκολο ως προς την πληρότητα, εγκυρότητα, και μηδενική γνώση τίμιου επαληθευτή (να εξεταστούν και οι τρεις ιδιότητες).

[Μονάδες: 15 (Μεταπτυχιακοί: 10)]

(γ΄) **Μόνο Μεταπτυχιακοί.** Στο μάθημα έχουμε δείξει ότι το πρωτόκολο του Schnorr επιτυγχάνει μηδενική γνώση μόνο απέναντι σε τίμιους επαληθευτές. Η παρακάτω σκιαγράφηση απόδειξης φέρεται να περιγράφει ένα Simulator μέσω του οποίου επιτυγχάνουμε μηδενική γνώση απέναντι σε οποιοδήποτε επαληθευτή $\mathcal{V}^*$.

> Το πρωτόκολο του Schnor επιτυγχάνει τέλεια μηδενική γνώση απέναντι σε οποιοδήποτε επαληθευτή $\mathcal{V}^*$. Προς τούτο, θα δώσουμε κατάληλο simulator πιθανοτικού πολυωνυμικού χρόνου $S_{\mathcal{V}*}$. Ο simulator $S_{\mathcal{V}*}$ εργάζεται ως εξής: επιλέγουμε τυχαία $c^*, s \leftarrow \mathbb{Z}_q$ και θέτουμε $y = g^s / h^{c^*}$. Εκκινούμε τον V^* με τυχαιότητα ρ και στέλνουμε το y. Εάν ο V^* επιστρέψει c^*, ολοκληρώνουμε επιτυχώς, διαφορετικά επαναλαμβάνουμε με νέα ρ, c^*, s. Για να ολοκληρώσουμε την απόδειξη, παρατηρούμε ότι όποτε ο S τερματίζει επιτυχημένα, η τριάδα y, c^*, s έχει την ίδια κατανομή με μια τριάδα $\bar{y}, \bar{c}, \bar{s}$ από μια πραγματική εκτέλεση.
>
> Συγκεκριμένα, το $y = g^s / h^{c*}$ είναι ομοιόμορφα κατανεμημένο στο $\langle g \rangle$ αφού το g^s είναι ομοιόμορφα κατανεμημένο στο $\mathbb{Z}_q$. Ομοίως το $\bar{y}$ ενός τίμιου Prover είναι της μορφής g^t και άρα επίσης ομοιόμορφα κατανεμημένο. Για τα $c^*, \bar{c}$ παρατηρούμε ότι $c^* = f_{\mathcal{V}^*}(y, \rho)$ και αντίστοιχα $\bar{c} = f_{\mathcal{V}^*}(\bar{y}, \rho)$, για κάποια συνάρτηση $f_{\mathcal{V}^*}$ που υπολογίζει ο $\mathcal{V}^*$ για δεδομένο ρ. Αφού οι κατανομές των $y, \bar{y}$ είναι ίδιες, ίδιες θα είναι και αυτές των $f_{\mathcal{V}^*}(y)$, $f_{\mathcal{V}^*}(\bar{y})$ δηλαδή των $c^*, \bar{c}$. Τέλος, επειδή γνωρίζουμε ότι για δεδομένα y, c υπάρχει μοναδικό s με το οποίο ένας verifier αποδέχεται, θα πρέπει να συμπίπτουν και οι κατανομές των $s, \bar{s}$, αφού το κάθε ένα είναι μοναδικό ως προς τα y, c^* και $\bar{y}, \bar{c}$ αντίστοιχα.

Εντοπίστε και εξηγήστε το λάθος στην παραπάνω απόδειξη.

[Μονάδες: 10 (Μόνο μεταπτυχιακοί)]

Όνομα: ΑΜ:

Θέμα 4. Εργαζόμαστε με το σύστημα κρυπτογράφησης ElGamal.

(α΄) Καλείστε να αξιολογήσετε τις παρακάτω πιθανές υλοποιήσεις της συνάρτησης GGen η οποία παράγει ομάδες για χρήση με το κρυπτοσύστημα ElGamal. Οι υλοποιήσεις χρησιμοποιούν τις συναρτήσεις `find_prime(n)` η οποία επιστρέφει ένα τυχαίο πρώτο αριθμο μήκους n bits, και `is_prime(p)` η οποία επιστρέφει 1 εάν ο p είναι πρώτος και 0 διαφορετικά. Οι απαιτήσεις μας για την GGen είναι να δέχεται ένα όρισμα λ, και να μας επιστρέφει μια τριάδα (p, q, g) που αναπαριστά μία ομάδα τάξης $q \approx 2^\lambda$, η οποία ορίζεται ως υποομάδα του $\mathbb{Z}_p^*$ και παράγεται από το g. Εάν το κρίνετε χρήσιμο, υποθέστε ότι $\lambda > 10$. Οι συναρτήσεις επιτρέπεται να αποτύχουν με κάποια πιθανότητα, στην οποία περίπτωση επιστρέφουν την ειδική τιμή (0,0,0).

function GGen-1(λ)
  $q \leftarrow$ `find_prime`(λ)
  $p \leftarrow 2q + 1$
  if `is_prime(p)` **then**
    $f \xleftarrow{r} \mathbb{Z}_p^*$
    $g \leftarrow (20f)^{19} \mod p$
    if $g \neq 1$ **then**
      Return (p,q,g)
    end if
  else
    Return (0,0,0)
  end if
end function

function GGen-2(λ)
  $q \leftarrow$ `find_prime`(λ)
  $p \leftarrow 2q + 1$
  if `is_prime(p)` **then**
    $f \xleftarrow{r} \mathbb{Z}_p^*$
    $g \leftarrow f^{20 \cdot 19} \mod p$
    if $g \neq 1$ **then**
      Return (p,q,g)
    end if
  else
    Return (0,0,0)
  end if
end function

function GGen-3(λ)
  $q \leftarrow$ `find_prime`(λ)
  $p \leftarrow 2q + 1$
  if `is_prime(p)` **then**
    $f \xleftarrow{r} \mathbb{Z}_p^*$
    $g \leftarrow ((2f)^0)^{19} \mod p$
    if $g \neq 1$ **then**
      Return (p,q,g)
    end if
  else
    Return (0,0,0)
  end if
end function

function GGen-4(λ)
  $q \leftarrow$ `find_prime`(λ)
  $p \leftarrow 2q + 1$
  if `is_prime(p)` **then**
    $f \xleftarrow{r} \mathbb{Z}_p^*$
    $g \leftarrow f^{2019} \mod p$
    if $g \neq 1$ **then**
      Return (p,q,g)
    end if
  else
    Return (0,0,0)
  end if
end function

Να επιλέξετε την καταλληλότερη από τις παραπάνω υλοποιήσεις, με πρώτο κριτήριο την ορθότητα, δεύτερο την ασφάλεια της ομάδας που επιλέγεται και ανάμεσα σε εξίσου σωστές και ασφαλείς υλοποιήσεις την αποδοτικότητα (χρόνος εκτέλεσης & επαναλήψεις λόγω αποτυχίας). Τεκμηριώστε την απαντησή σας (ως προς την υλοποίηση που επιλέξατε και ως προς αυτές που απορρίψατε).

[Μονάδες: 10]

(β΄) Θέλουμε να εξετάσουμε την ασφάλεια του συστήματος ElGamal σε συνθήκες δυσκολότερες από αυτές του πειράματος IND-CPA. Συγκεκριμένα, θέλουμε να δώσουμε την εξής δυνατότητα στον αντίπαλο: πριν μαντέψει τον δείκτη του μηνύματος που βρίσκεται στο κρυπτογράφημα c, στέλνει στο πείραμα ένα κρυπτογράφημα c^* της επιλογής του. Το πείραμα επιστρέφει την αποκρυπτογράφηση του, εκτός αν ισχύει ότι $c^* = c$ στην οποία περίπτωση στέλνει $\perp$.

Διατυπωστε πλήρως το πείραμα και τον τον ορισμό ασφάλειας που προκύπτει από τις παραπάνω αλλαγές.

[Μονάδες: 10]

(γ΄) Εξετάστε αν το σύστημα ElGamal είναι ασφαλές ως προς τον παραπάνω ορισμό.

[Μονάδες: 10]

Καλή Επιτυχία